Certified Wireless Analysis Professional

CWNP CWAP-404

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, 802.11 Physical (PHY) Layer Analysis	8
Topic 2, 802.11 MAC Layer Analysis	42
Topic 3, WLAN Security Analysis	12
Topic 4, Spectrum Analysis	10
Topic 5, WLAN Analysis and Troubleshooting	8
Total	80

QUESTION NO: 1

You are investigating intermittent performance problems on a 2.4 GHz WLAN. A swept spectrogram shows short bursts of energy that repeatedly move across much of the 2.4 GHz band rather than remaining on one fixed frequency. Which type of RF behavior is most strongly suggested by this observation?

A. Frequency-hopping RF activity

B. A fixed-frequency narrowband interferer

C. An AP transmitting only on its primary 20 MHz channel

D. A client using a hidden SSID

ANSWER: A

Explanation:

The pattern most strongly suggests a frequency-hopping transmitter. A swept spectrogram displays RF power by frequency over time, so repeated short-duration energy bursts that move among frequencies are characteristic of devices that change operating frequencies as part of their transmission behavior, such as Bluetooth-class frequency-hopping activity.

The display alone does not prove the exact device type, but it distinguishes hopping behavior from a fixed-frequency interferer. A persistent fixed-frequency source would remain concentrated in the same spectral region, while normal 802.11 activity generally follows the configured WLAN channel widths rather than hopping across the band in this manner.

QUESTION NO: 2

Where, in a protocol analyzer, would you find an indication that a frame was transmitted as part of an A-MPDU?

A. The HT Operation Element

B. A-MPDU flag in the QoS Control Field

C. A-MPDU flag in the Frame Control Field

D. The Aggregation flag in the Radio Tap Header

ANSWER: D

Explanation:

The Aggregation flag in the Radio Tap Header is the correct location because A-MPDU membership is capture metadata supplied by the wireless adapter and driver to the protocol analyzer. An A-MPDU is a PHY-layer transmission containing multiple independently formed MPDUs, so an individual decoded 802.11 MAC frame does not carry a normal MAC-header bit that directly declares it was transmitted within an aggregate. When the capture hardware/driver can report aggregation information, it places that information in the radiotap pseudo-header associated with the captured frame. Wireshark and similar analyzers can then display the metadata to show that a received MPDU belonged to an A-MPDU, often along with related aggregate-status details such as reference information or delimiter status. This is especially useful during WLAN troubleshooting because it lets the analyst distinguish normal individual transmissions from traffic delivered as part of high-throughput or very-high-throughput aggregation. The radiotap specification defines an A-MPDU-status field for this type of metadata; implementations and training material may describe the relevant indication generically as an aggregation flag. See the radiotap A-MPDU status field definition and Wireshark's wlan_radio dissector field reference.

QUESTION NO: 3

You are examining a data frame transmitted between two APs across a wireless distribution system. The frame has both the To DS and From DS flags set to 1. Which address field identifies the original source STA?

A. Address 1

B. Address 2

C. Address 3

D. Address 4

ANSWER: D

Explanation:

Address 4 identifies the original source STA when both the To DS and From DS flags are set to 1. This combination indicates a four-address frame format, which is used for wireless distribution system forwarding. In this format, Address 1 is the receiver address, Address 2 is the transmitter address, Address 3 is the destination address, and Address 4 is the source address. The transmitter and receiver are the APs participating in the wireless hop, while the destination and source identify the end stations communicating through that hop.

Address 2 identifies the AP that transmitted the frame over the current wireless link, not the original source STA. Address 3 identifies the final destination, and the BSSID is not carried in the normal infrastructure-frame role when both DS bits are set.

QUESTION NO: 4

During a VHT Transmit Beamforming sounding exchange, the beamformee transmits a Compressed Beamforming frame to the beamformer. What is communicated within this Compressed Beamforming frame?

A. Steering Matrix

B. Beamforming Matrix

C. Feedback Matrix

D. Beamformee Matrix

ANSWER: C

Explanation:

Feedback Matrix is correct. In a VHT transmit-beamforming sounding procedure, the beamformer first sends a sounding sequence so that the beamformee can measure the RF channel from the beamformer's transmit chains to its receive chains. The beamformee then returns a VHT Compressed Beamforming action frame containing compressed channel-state feedback. Its Compressed Beamforming Report field includes the feedback matrices, conventionally represented as angle information that describes the channel's spatial characteristics across the reported subcarriers and spatial streams. The report can also include the channel-quality indicator used by the beamformer when selecting transmission characteristics. The beamformer uses this feedback to derive transmit steering weights that spatially focus its VHT transmission toward that particular beamformee. Because explicit beamforming depends on the receiving station measuring and reporting the observed channel, this feedback matrix is the essential information communicated from beamformee to beamformer during the sounding exchange. The 802.11 specification defines VHT compressed beamforming feedback and its report fields; CWNP's CWAP curriculum covers analysis of these PHY and beamforming exchanges. See IEEE 802.11 standard information and CWNP CWAP certification.

QUESTION NO: 5

What is the difference between a Data frame and a QoS-Data frame?

A. QoS Data frames include a DSCP control field

B. QoS Data frames include a QoS information element

C. QoS Data frames include an 802.1Q VLAN tag

D. QoS Data frames include a QoS control field

ANSWER: D

Explanation:

QoS Data frames include a QoS control field. In the IEEE 802.11 MAC frame format, QoS Data is a Data-frame subtype defined for stations using Enhanced Distributed Channel Access (EDCA) under 802.11e quality-of-service operation. The QoS Control field is present in the MAC header of QoS Data frames, immediately following the optional Address 4 field when that field is present. Its Traffic Identifier subfield identifies the user priority and traffic category used for EDCA handling. Other subfields support QoS behavior such as acknowledgement policy, transmission opportunity considerations, and—in applicable frame contexts—queue-size or power-management information. This explicit MAC-layer control information lets wireless devices classify and handle traffic according to its service requirements, such as prioritizing latency-sensitive voice or video traffic over best-effort traffic. A non-QoS Data frame does not contain this QoS Control field. The 802.11 frame-type and subtype definitions, including QoS Data, are maintained by the IEEE 802.11 working group; see the IEEE 802.11 Working Group. For a practical overview of Wi-Fi QoS operation and the traffic categories that use QoS Data frames, see Cisco Wireless Controller QoS Configuration Guide.

QUESTION NO: 6

In the 2.4 GHZ band, what data rate are Probe Requests usually sent at from an unassociated STA?

A. 1 Mbps

B. The minimum basic rate

C. MCS 0

D. 6 Mbps

ANSWER: A

Explanation:

1 Mbps is correct because an unassociated station performing active scanning in the 2.4 GHz band normally transmits its broadcast Probe Request at the lowest legacy DSSS rate, 1 Mbps. At this point, the station has not joined a BSS and therefore cannot rely on the basic-rate configuration advertised by any particular access point. Using 1 Mbps maximizes the likelihood that nearby 2.4 GHz access points and stations can decode the management frame, including older 802.11b-capable devices. This low-rate transmission also gives the broadcast management frame greater range than a higher-rate transmission, helping the client discover BSSs that may be farther away.

After receiving Probe Responses and selecting a BSS, the station obtains the applicable supported and basic-rate information from management-frame information elements and then communicates according to that BSS's capabilities and policies. The scanning behavior described here is specifically a common legacy-rate behavior for 2.4 GHz active scanning; it should not be generalized to every band or every modern client implementation. CWAP analysis requires recognizing the practical distinction between a station that is already associated and one that is still discovering candidate networks. See the CWNP CWAP certification overview and the Wi-Fi Alliance overview of 802.11n-era Wi-Fi for related WLAN technology context.

QUESTION NO: 7

Prior to a retransmission what happens to the CWmax value?

A. Increases by 1

B. Reset to 0

C. Set to the value of the AIFSN

D. Doubles and increases by 1

E. The current CW doubles and increases by 1, up to CWmax; CWmax itself is unchanged.

ANSWER: E

Explanation:

The current contention-window value is doubled and increased by 1, up to the configured CWmax; CWmax itself is unchanged. In IEEE 802.11 CSMA/CA, a station that has an unsuccessful transmission attempt—such as one not acknowledged—uses binary exponential backoff before retrying. Its current CW is updated according to the equivalent expression $CW_{new} = \min(2 \times CW_{old} + 1, CWmax)$. The station then randomly selects a new backoff counter from the range beginning at zero through that updated current CW. Increasing the current window expands the selection range and reduces the probability that contending stations will choose the same backoff value again. CWmax is instead a configured ceiling on this growth, commonly defined separately for each EDCA access category along with CWmin and AIFSN. Once the calculated current CW reaches CWmax, further failed attempts retain that ceiling rather than changing the CWmax parameter. This distinction between the dynamic current CW and the fixed CWmax limit is essential when interpreting retry behavior in packet captures and QoS analysis. See the IEEE 802.11 working-group standard information at IEEE 802.11 and CWNP's CWAP certification overview.

QUESTION NO: 8

Where would you look in a packet trace file to identify the configured Minimum Basic Rate (MBR) of a BSS?

A. Supported Rates & Extended Supported Rates elements in a Beacon frame

B. In the MBR Action frame

C. In the MBR Information Element in an Association Response frame

D. In the Minimum Basic Rate Element in a Beacon frame

ANSWER: A

Explanation:

The configured Minimum Basic Rate is identified from the Supported Rates and Extended Supported Rates information elements carried in Beacon management frames. These elements advertise the PHY data rates available in the BSS. Each advertised rate is encoded in units of 500 kb/s, and the most significant bit of each rate octet is the Basic Rate flag. Rates with that flag set form the BSS basic-rate set; the lowest of those marked rates is the Minimum Basic Rate. A packet analyst can therefore expand the Beacon frame's tagged parameters in a decoder such as Wireshark, inspect both rate elements when present, and find the lowest rate designated as basic. Both elements must be considered because the Supported Rates element has limited space and additional advertised rates can appear in Extended Supported Rates. Beacon frames are especially useful because APs transmit them periodically, allowing the rate configuration to be observed without relying on a client association exchange. This interpretation follows the 802.11 management-frame rate-set encoding and practical WLAN packet-analysis methodology. See the Wireshark IEEE 802.11 management-field reference and CWNP's CWAP certification overview.